IEC 61139-2

Edition 1.0 2022-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial networks – Single-drop digital communication interface – Part 2: Functional safety extensions

Réseaux industriels – Interface de communication numérique point à point – Partie 2: Extensions de sécurité fonctionnelle

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040

ISBN 978-2-8322-3946-9

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

CONTENTS

FOREWORD 12
INTRODUCTION 14
1 Scope 17
2 Normative references 17
3 Terms, definitions, symbols, abbreviated terms, and conventions 18
3.1 Terms and definitions 18
3.2 Common terms and definitions 18
3.3 Terms and definitions related to SDCI-FS 21
3.4 Symbols and abbreviated terms 23
3.5 Conventions 24
3.5.1 Behavioral descriptions 24
3.5.2 Memory and transmission octet order 25
4 Overview of SDCI-FS 25
4.1 Purpose of the technology and feature levels 25
4.1.1 Base SDCI-FS technology 25
4.1.2 From "analog" and "switching" to communication 26
4.1.3 Minimized paradigm shift from FS-DI to FS-Master 27
4.1.4 Following the SDCI paradigm (SIO vs. OSSDe) 28
4.1.5 Port class B 30
4.1.6 "USB-Master" with safety parameterization 31
4.1.7 Interoperability matrix of safety devices 31
4.2 Positioning within the automation hierarchy 32
4.3 Wiring, connectors, and power supply 33
4.4 Relationship to SDCI 33
4.5 Communication features and interfaces 34
4.6 Parameterization 34
4.7 Role of FS-Master and FS-Gateway 35
4.8 Mapping to upper-level systems 35
4.9 Structure of the document 35
5 Extensions to the Physical Layer (PL) 35
5.1 Overview 35
5.2 Extensions to PL services 36
5.2.1 PL_SetMode 36
5.2.2 PL_Ready 36
5.3 Transmitter/receiver 37
5.3.1 Assumptions for the expansion to OSSDe 37
5.3.2 OSSDe specifics 37
5.3.3 Start-up of an FS-Device (Ready pulse) 40
5.3.4 Electric characteristics of a receiver in FS-Device and FS-Master 41
5.4 Electric and dynamic characteristics of an FS-Device 41
5.5 Electric and dynamic characteristics of an FS-Master port (OSSDe) 44
5.6 FS-Master port FS-DI interface 45
5.7 Wake-up coordination 45
5.8 Fast start-up 46
5.9 Power supply 46
5.10 Medium 47

5.10.1 Constraints 47
5.10.2 Connectors 47
5.10.3 Cable characteristics 47
6 Extensions to SIO 47
7 Extensions to the data link layer (DL) 47
7.1 Overview 47
7.2 State machine of the FS-Master DL-mode handler 47
7.3 State machine of the FS-Device DL-mode handler 49
8 Extensions to the Master Configuration Manager (CM) 51
9 Extensions of the FS-Device 52
9.1 Principle architecture and models 52
9.1.1 FS-Device architecture 52
9.1.2 FS-Device model 53
9.2 Parameter Manager (PM) 54
9.3 Process Data Exchange (PDE) 54
9.4 Data Storage (DS) 54
9.4.1 General considerations and extensions including safety 54
9.4.2 Backup levels 55
10 Extensions of the FS-Master 55
10.1 Principle architecture 55
10.2 SMI service extensions 56
10.2.1 Overview 56
10.2.2 SMI_FSMasterAccess 58
10.2.3 SMI_SPDUIn 60
10.2.4 SMI_SPDUOut 60
10.2.5 SMI_FSPDInOut 60
10.3 ArgBlock extensions 62
10.3.1 Overview 62
10.3.2 FSMasterAccess 62
10.3.3 FSCPAuthenticity 63
10.3.4 FSPortConfigList 63
10.3.5 FSPortStatusList 66
10.3.6 SPDUIn 67
10.3.7 SPDUOut 67
10.3.8 FSPDInOut 68
10.4 Safety Layer Manager (SLM) 69
10.4.1 Purpose 69
10.4.2 FS_PortModes 69
10.4.3 FSP parameter 69
10.5 Process Data Exchange (PDE) 73
10.6 Data Storage (DS) 74
11 Safety communication layer (SCL) 74
11.1 Functional requirements 74
11.2 Communication errors and safety measures 74
11.3 SCL services 75
11.3.1 Positioning of safety communication layers (SCL) 75
11.3.2 FS-Master SCL services 76
11.3.3 FS-Device SCL services 77

11.4 SCL protocol 79
11.4.1 Protocol phases to consider 79
11.4.2 FS-Device faults 80
11.4.3 Safety PDU (SPDU) 80
11.4.4 FS-Input and FS-Output data 81
11.4.5 Port number 81
11.4.6 Status and control 81
11.4.7 CRC signature 82
11.4.8 TADI safety considerations (informative) 83
11.4.9 Data types for SDCI-FS 84
11.5 SCL behavior 85
11.5.1 General 85
11.5.2 SCL state machine of the FS-Master 85
11.5.3 SCL state machine of the FS-Device 88
11.5.4 Sequence charts for several use cases 91
11.5.5 Monitoring of safety times 98
11.5.6 Reaction in the event of a malfunction 99
11.5.7 Start-up (communication) 101
11.6 SCL management 101
11.6.1 Parameter overview (FSP and FST) 101
11.6.2 Parameterization approaches 103
11.7 Integrity measures 104
11.7.1 IODD integrity 104
11.7.2 Tool integrity 104
11.7.3 Transmission integrity 104
11.7.4 Verification record 104
11.7.5 Authentication 105
11.7.6 Storage integrity 105
11.7.7 FS I/O data structure integrity 106
11.7.8 Technology parameter (FST) based on IODD 106
11.7.9 Technology parameter (FST) based on existing Dedicated Tool (IOPD) 107
11.8 Creation of FSP and FST parameters 108
11.9 Integration of Dedicated Tools (IOPD) 109
11.9.1 IOPD interface 109
11.9.2 Standard interfaces 109
11.9.3 Backward channel 110
11.10 Validation 111
11.11 Passivation 111
11.11.1 Motivation and means 111
11.11.2 Port selective (FS-Master) 111
11.11.3 Signal selective (FS-Terminal) 112
11.11.4 Qualifier settings in case of communication 112
11.11.5 Qualifier handling in case of OSSDe 112
11.12 SCL diagnosis 113
12 Functional safe processing (FS-P) 114
12.1 Recommendations for efficient I/O mappings 114
12.2 Embedded FS controller 114
Annex A (normative) Extensions to parameters 115
A.1 Indices and parameters for SDCI-FS 115

A.2 Parameters in detail 116
A.2.1 FSP_Authenticity 116
A.2.2 FSP_Port 116
A.2.3 FSP_AuthentCRC 117
A.2.4 FSP_ProtVersion 117
A.2.5 FSP_ProtMode 117
A.2.6 FSP_Watchdog 117
A.2.7 FSP_IO_StructCRC 118
A.2.8 FSP_TechParCRC 119
A.2.9 FSP_ProtParCRC 119
A.2.10 FSP_VerifyRecord 119
A.2.11 FSP_TimeToReady 119
A.2.12 FSP_MinShutDownTime 120
A.2.13 FSP_WCDT 120
A.2.14 FSP_OFDT 120
A.2.15 FSP_ParamDescCRC 120
Annex B (normative) Extensions to EventCodes 121
B.1 Additional FS-Device EventCodes 121
B.2 Additional Port EventCodes 121
Annex C (normative) Extensions to Data Types 123
C.1 Data types for SDCI-FS 123
C.2 BooleanT (bit) 123
C.3 IntegerT (16) 124
C.4 IntegerT (32) 124
C.5 Safety Code 125
Annex D (normative) CRC generator polynomials 126
D.1 Overview of CRC generator polynomials 126
D.2 Residual error probabilities 126
D.3 Implementation considerations 128
D.3.1 Overview 128
D.3.2 Bit shift algorithm (16 bit) 128
D.3.3 Lookup table (16 bit) 128
D.3.4 Bit shift algorithm (32 bit) 130
D.3.5 Lookup table (32 bit) 130
D.3.6 Seed values 131
D.3.7 Octet order for CRC calculation 132
Annex E (normative) IODD extensions 133
E.1 General 133
E.2 Schema 133
E.3 IODD constraints 133
E.3.1 General rules 133
E.3.2 Description of the IODD structure 133
E.3.3 Behavior of "Reset" SystemCommands in SDCI-FS 140
E.3.4 Profile Characteristic 141
E.3.5 ProcessDataInput and ProcessDataOutput 141
E.4 IODD conventions 141
E.4.1 Naming 141
E.4.2 Process Data (PD) 141

E.4.3 IODD conventions for user interface 142
E.4.4 Master Tool features 142
E.5 Securing 142
E.5.1 General 142
E.5.2 DefaultValues for FSP 143
E.5.3 FSP_Authenticity 143
E.5.4 FSP_Protocol 143
E.5.5 FSP_IO_Description 144
E.5.6 Sample serialization for FSP_ParamDescCRC 144
E.5.7 FST and FSP parameters and Data Storage 145
E.5.8 Sample IODD of an FS-Device 145
Annex F (normative) Device Tool Interface (DTI) for SDCI 156
F.1 Purpose of DTI 156
F.2 Base model 156
F.3 Invocation interface 157
F.3.1 Overview 157
F.3.2 Detection of Device Tool 158
F.3.3 Program Interface Description – PID 161
F.3.4 Temporary Parameter File – TPF 164
F.3.5 Temporary Backchannel File – TBF 169
F.3.6 Temporary Acknowledgment File – TAF 171
F.3.7 Invocation behavior 171
F.4 Device data objects (DDO) 172
F.4.1 General 172
F.4.2 Structure of DDO package 173
F.5 Communication Interface 173
F.5.1 General 173
F.5.2 Principle of DTI communications 174
F.5.3 Gateways 175
F.5.4 Configuration of the Communication Server 175
F.5.5 Definition of the Communication Interface 176
F.5.6 Sequence for establishing a communication relation 176
F.5.7 Usage of the Communication Server in stand-alone mode 177
F.5.8 SDCI specifics 178
F.5.9 Changing communication settings 178
F.6 Reaction on incorrect Tool behavior 179
F.7 Compatibility 179
F.7.1 Schema validation 179
F.7.2 Version policy 180
F.8 Scalability 180
F.8.1 Scalability of a Device Tool 180
F.8.2 Scalability of a Master Tool 181
F.8.3 Interactions at conformance class combinations 181
F.9 Schema definitions 181
F.9.1 General 181
F.9.2 Schema of the PID 181
F.9.3 Schema of the TPF 183
F.9.4 Schema of the TBF 185
F.9.5 Schema of the TAF 186

F.9.6 Schema of DTI primitives 187
Annex G (normative) Main scenarios of SDCI-FS 189
G.1 Overview 189
G.2 Sequence chart of commissioning 190
G.3 Sequence chart of replacement 191
G.4 Sequence chart of misconnection 192
Annex H (normative) System requirements 193
H.1 Indicators 193
H.1.1 General 193
H.1.2 OSSDe 193
H.1.3 Safety communication 193
H.1.4 Acknowledgment request 193
H.2 Installation guidelines, electrical safety, and security 193
H.3 Safety function response time 194
H.4 Duration of demands 194
H.5 Maintenance and repair 194
H.6 Safety manual 194
Annex I (informative) Information for test and assessment of SDCI-FS components 195
Bibliography 196

Figure 1 – Positioning of SDCI-FS in functional safety automation 14
Figure 2 – Relationship of this document to standards 16
Figure 3 – Memory and transmission octet order 25
Figure 4 – SDCI-FS communication layer model 25
Figure 5 – Port interface extensions for SDCI-FS 26
Figure 6 – Migration to SDCI-FS 27
Figure 7 – Minimized paradigm shift from FS-DI to FS-Master 28
Figure 8 – FS-Master types and feature levels 28
Figure 9 – Original pin layout of SDCI (port class A) 29
Figure 10 – Optimized OSSDe commissioning with FS-Master 30
Figure 11 – Level "d" of an FS-Master (Class B) 31
Figure 12 – Off-site configuration and parameterization 31
Figure 13 – SDCI-FS within the automation hierarchy 33
Figure 14 – The SDCI physical layer of an FS-Master (class A) 36
Figure 15 – The physical layer of an FS-Device (class A) 36
Figure 16 – Cross compatibility OSSD and OSSDe 37
Figure 17 – Principle OSSDe function 38
Figure 18 – Test pulses to detect cross connection faults 39
Figure 19 – OSSD timings 40
Figure 20 – Typical start-up of an OSSD sensor 40
Figure 21 – Start-up of an FS-Device 40
Figure 22 – Switching thresholds for FS-Device and FS-Master receivers 41
Figure 23 – Reference schematics (one OSSDe channel) 42
Figure 24 – Voltage level definitions 42
Figure 25 – Charge capability at power-up 45

Figure 26 – OSSDe input filter conflict resolution 45
Figure 27 – Start-up of an FS-Device 46
Figure 28 – Required fast start-up timings 46
Figure 29 – State machine of the FS-Master DL-mode handler 48
Figure 30 – State machine of the FS-Device DL-mode handler 50
Figure 31 – Extension to the Configuration Manager (VerifyRecord) 51
Figure 32 – Principle architecture of the FS-Device 53
Figure 33 – The FS-Device model 54
Figure 34 – Principle architecture of the FS-Master 56
Figure 35 – SMI service extensions 58
Figure 36 – FSP parameter use cases 70
Figure 37 – PDE Splitter 73
Figure 38 – PDE Composer 74
Figure 39 – Positioning of the SDCI-FS Safety Communication Layer (SCL) 76
Figure 40 – FS-Master Safety Communication Layer services 76
Figure 41 – FS-Device Safety Communication Layer services 78
Figure 42 – Protocol phases to consider 79
Figure 43 – Safety PDUs of FS-Master and FS-Device 80
Figure 44 – The 1 % share rule of IEC 61784-3:2021 83
Figure 45 – SCL state machine of the FS-Master 86
Figure 46 – SCL state machine of the FS-Device 89
Figure 47 – FS-Master and FS-Device both with power ON 92
Figure 48 – FS-Master power OFF → ON 93
Figure 49 – FS-Device with delayed SCL start 94
Figure 50 – FS-Device with power OFF and ON 95
Figure 51 – FS-Master detects CRC signature error 96
Figure 52 – FS-Device detects CRC signature error 97
Figure 53 – Monitoring of the SCL cycle time 98
Figure 54 – Parameter types and assignments 102
Figure 55 – FSCP-Host-centric system 103
Figure 56 – Structure of the FSP_VerifyRecord 105
Figure 57 – Start-up of SDCI-FS 106
Figure 58 – Securing of FST parameters via dedicated tool 107
Figure 59 – Modification of FST parameters via Device Tool 108
Figure 60 – Creation of FSP and FST parameters 109
Figure 61 – Example of a communication hierarchy 110
Figure 62 – Motivation for Port selective passivation 111
Figure 63 – Qualifier handler (communication) 112
Figure 64 – Qualifier handler (OSSDe) 112
Figure 65 – Qualifier behavior per FS-Master port 113
Figure 66 – Mapping efficiency issues 114
Figure A.1 – Instance of an FS I/O data description 118
Figure A.2 – Example FS I/O data structure with non-safety data 119

Figure A.3 – Securing of safety parameters 120
Figure C.1 – Example of a BooleanT data structure 124
Figure C.2 – Safety Code of an output message 125
Figure C.3 – Safety Code of an input message 125
Figure D.1 – CRC-16 generator polynomial 127
Figure D.2 – CRC-32 generator polynomial 127
Figure D.3 – Bit shift algorithm in "C" language (16 bit) 128
Figure D.4 – CRC-16 signature calculation using a lookup table 128
Figure D.5 – Bit shift algorithm in "C" language (32 bit) 130
Figure D.6 – CRC-32 signature calculation using a lookup table 130
Figure E.1 – Algorithm to build the FSP parameter CRC signatures 143
Figure F.1 – Principle of DTI invocation interface 157
Figure F.2 – Structure of the registry 158
Figure F.3 – Example of a DTI registry 159
Figure F.4 – Detection of a Device tool in registry 161
Figure F.5 – Menu for Device Tool invocation 162
Figure F.6 – Purpose of Device data objects (DDO) 173
Figure F.7 – Communication routes between Device Tool and Device 174
Figure F.8 – Routing across networks and SDCI 174
Figure F.9 – Communication Server 175
Figure F.10 – Sequence chart for establishing communication 176
Figure F.11 – Create Communication Server instance 177
Figure F.12 – Example of a Connect Request XML document for SDCI 178
Figure F.13 – XML schema of the PID file 181
Figure F.14 – XML schema of the TPF 183
Figure F.15 – XML schema of a TBF 185
Figure G.1 – Commissioning with test and armed operation 191
Figure G.2 – FS-Device replacement 192
Figure G.3 – FS-Device misconnection 192

Table 1 – Operational modes of feature level "a" to "c" (port class A) 30
Table 2 – Interoperability matrix of safety devices 32
Table 3 – PL_Ready 36
Table 4 – OSSD states and conditions 38
Table 5 – Cross connection faults 39
Table 6 – Electric characteristics of a receiver 41
Table 7 – Electric and dynamic characteristics of the FS-Device (OSSDe) 43
Table 8 – Electric and dynamic characteristics of the Port interface 44
Table 9 – Cable characteristics 47
Table 10 – State transition tables of the FS-Master DL-mode handler 49
Table 11 – State transition tables of the FS-Device DL-mode handler 50
Table 12 – State transition tables of the Configuration Manager 52
Table 13 – Extension to Data Storage (DS) state machine 55

Table 14 – Data Storage Backup Levels 55
Table 15 – SMI services used for FS-Master 57
Table 16 – SMI_FSMasterAccess 59
Table 17 – SMI_FSPDInOut 61
Table 18 – ArgBlock types and ArgBlockIDs 62
Table 19 – FSMasterAccess 63
Table 20 – FSCPAuthenticity 63
Table 21 – FSPortConfigList 64
Table 22 – FSPortStatusList 66
Table 23 – SPDUIn 67
Table 24 – SPDUOut 68
Table 25 – FSPDInOut 68
Table 26 – Use case reference table 70
Table 27 – Communication errors and safety measures 75
Table 28 – SCL services of FS-Master 77
Table 29 – SCL services of FS-Device 78
Table 30 – Protocol phases to consider 80
Table 31 – Control and counting (Control&MCnt) 81
Table 32 – Status and counting mirror (Status&DCnt) 81
Table 33 – MCount and DCount_i values 82
Table 34 – FS process I/O data types 84
Table 35 – Rules for the layout of values and qualifiers 84
Table 36 – Order of values and qualifier 85
Table 37 – Definition of terms used in SCL state machine of the FS-Master 86
Table 38 – FS-Master SCL states and transitions 87
Table 39 – Definition of terms used in SCL state machine of the FS-Device 89
Table 40 – FS-Device SCL states and transitions 90
Table 41 – Timing constraints 98
Table 42 – Qualifier bits "GOOD/BAD" 112
Table 43 – State transition Table for the qualifier behavior 113
Table A.1 – Indices for SDCI-FS 115
Table A.2 – Coding of protocol version 117
Table A.3 – Coding of protocol mode 117
Table A.4 – Generic FS I/O data structure description 118
Table B.1 – FS-Device SCL specific EventCodes 121
Table B.2 – FS-Master SCL specific EventCodes 122
Table C.1 – Data types for SDCI-FS 123
Table C.2 – BooleanT for SDCI-FS 123
Table C.3 – Example of BooleanT within a RecordT 123
Table C.4 – IntegerT(16) 124
Table C.5 – IntegerT(16) coding 124
Table C.6 – IntegerT(32) 125
Table C.7 – IntegerT(32) coding 125

Table D.1 – CRC generator polynomials for SDCI-FS 126
Table D.2 – Definition of variables used in Figure D.3 128
Table D.3 – Definition of variables used in Figure D.4 129
Table D.4 – Lookup Table for CRC-16 signature calculation 129
Table D.5 – Definition of variables used in Figure D.5 130
Table D.6 – Definition of variables used in Figure D.4 130
Table D.7 – Lookup Table for CRC-32 signature calculation 131
Table E.1 – Specific behavior of FS-Device "Reset" SystemCommands 141
Table E.2 – User actions to replace DefaultValues 143
Table E.3 – RecordItems of FSP_Protocol where allowed values shall be serialized 144
Table E.4 – Sample serialization for FSP_ParamDescCRC 144
Table F.1 – Description of PID file elements 162
Table F.2 – Elements of a TPF 165
Table F.3 – Elements of the TBF 170
Table F.4 – Elements of the TAF 171
Table F.5 – Invocation cases and behaviors 172
Table F.6 – Communication Schema mapping 178
Table F.7 – Reaction on incorrect Tool behavior 179
Table F.8 – DTI conformance classes 180
Table F.9 – DTI feature levels of Device Tools 180
Table F.10 – Interactions at conformance class combinations 181
Table G.1 – Main scenarios of SDCI-FS 189

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

INDUSTRIAL NETWORKS – SINGLE-DROP DIGITAL COMMUNICATION INTERFACE –

Part 2: Functional safety extensions

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 61139-2 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee TC65: Industrial-process measurement, control and automation. It is an International Standard.

The text of this International Standard is based on the following documents:

Draft	Report on voting
65C/1168/FDIS	65C/1174/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

A list of all parts in the IEC 61139 series, published under the general title *Industrial networks – Single-drop digital communication interface*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

The base technology of IO-Link™ [1] is subject matter of the international standard IEC 61131-9 being part of a series of standards on programmable controllers and the associated peripherals such as remote I/O (RIO).

It specifies a single-drop digital communication interface technology – named SDCI, which extends the traditional switching input and output interfaces as defined in IEC 61131-2 towards a point-to-point communication link using coded switching. This technology enables the cyclic exchange of digital input and output process data between a Master and its associated Devices (sensors, actuators, I/O terminals, etc.). The Master can be part of a fieldbus communication system or any stand-alone processing unit. The technology also enables the acyclic transfer of parameters to Devices and the propagation of diagnosis information from the Devices to the upper-level automation system (controller, host) via the Master.

Physical topology is point-to-point from each Device to the Master using 3 wires over distances up to 20 m. The SDCI physical interface is backward compatible with the usual 24 V I/O signalling specified in IEC 61131-2 and supports three transmission rates of 4,8 kbit/s, 38,4 kbit/s and 230,4 kbit/s are supported.

The main advantages of the SDCI technology are:

- dual use of either switching signals (DI/DO) or coded switching communication respectively,
- traditional switching sensors and actuators now providing alternatively single drop digital communication within the same Device,
- one thin, robust, very flexible cable without shielding for power supply and signalling,
- lowest-cost digital communication down to the lowest end sensors and actuators.

The functional safety variant of SDCI is called SDCI-FS. Figure 1 shows an example positioning of SDCI-FS in functional safety automation.

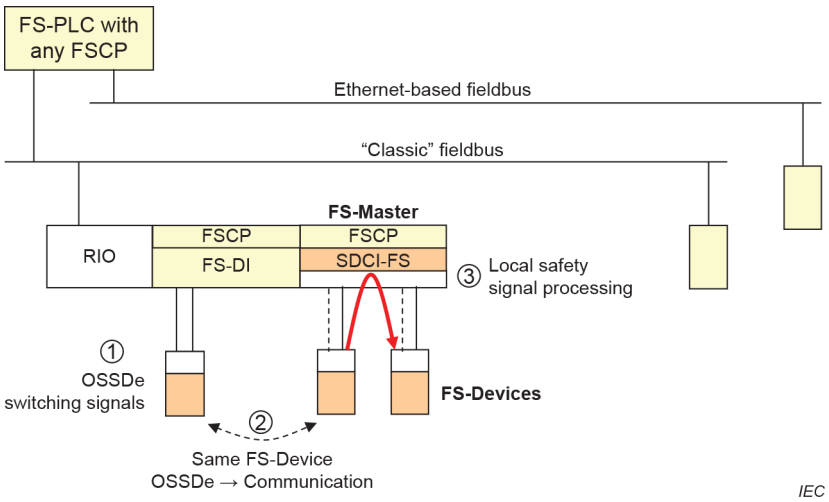


Figure 1 – Positioning of SDCI-FS in functional safety automation

[1] IO-Link™ is a trade name of the "IO-Link Community". This information is given for the convenience of users of this specification and does not constitute an endorsement by the IO-Link Community of the trade name holder or any of its products. Compliance to this document does not require use of the registered logos for IO-Link™. Use of the registered logos for IO-Link™ requires permission of the "IO-Link Community".

In this example, a remote I/O is connected to a functional safety programmable controller using one of the FSCPs of the IEC 61784-3 series [1][2] to communicate with an FS-DI module and a gateway to an SDCI-FS FS-Master. FS-Devices with OSSDe can be connected to FS-DIs or FS-Masters. All FS-Devices can communicate with any FS-Master using the SDCI-FS protocol regardless of the upper-level FSCP-system. The same is true for safety actuators (FS-Devices) such as drives with integrated safety. This means the largest component commonality ① for sensors and actuators similar to the DI and DO interfaces standardized within IEC 61131-2.

Safety sensors with OSSDe interfaces – equipped with SDCI-FS communication – can be parameterized via auxiliary tools such as "USB-Masters", then connected to an FS-DI and operated in OSSDe mode. They also can be operated in OSSDe mode on an FS-Master that supports OSSDe. In case these safety sensors are equipped with SDCI-FS communication in addition, they can be operated in both modes ②, either OSSDe or SDCI-FS. This corresponds to the SDCI SIO paradigm.

The concept of SDCI-FS allows for local safety signal processing if the gateway/FS-Master provides a local safety controller ③.

This document provides the necessary extensions to IEC 61131-9 for functional safety communication including standardization of OSSDe and parameterization within the domain of safety for machinery. Figure 2 shows its relationships to international fieldbus and safety standards as well as to relevant specifications (see Clause 2 and bibliography). Any functional safety starts with risk assessment and risk reduction (ISO 12100). One possibility of risk reduction is the usage of electrical or electronic control systems. For the design of those, standards such as IEC 61508, IEC 62061, and ISO 13849 can be used. Environmental conditions such as EMC are covered by for example IEC 61000-6-7. Further aspects are installations and security issues. A number of product standards such as IEC 60947-5-3 and ISO 14119 complement the generic or sector standards.

[2] Numbers in square brackets refer to the Bibliography.

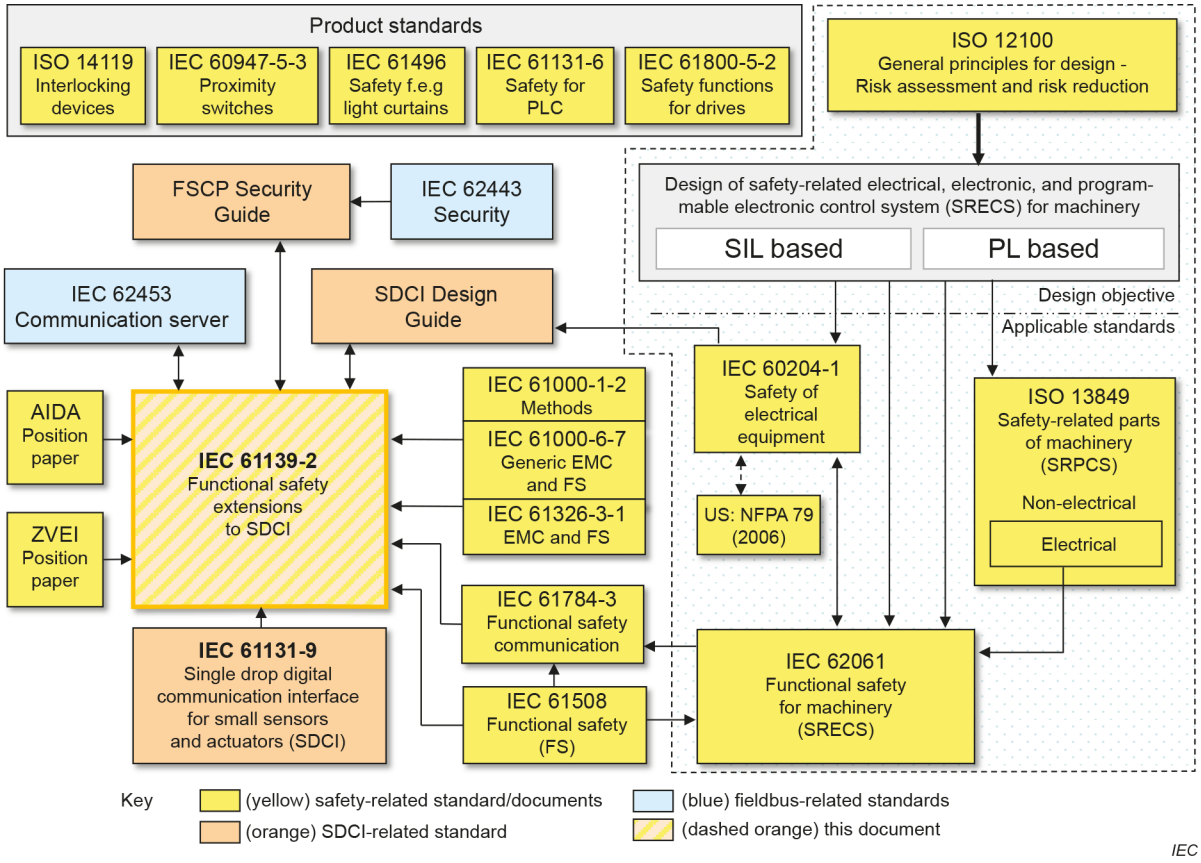


Figure 2 – Relationship of this document to standards

SDCI-FS can be used for functional safety applications according to IEC 62061 and IEC 61508 up to SIL3 and/or according to ISO 13849 up to PLe.

INDUSTRIAL NETWORKS – SINGLE-DROP DIGITAL COMMUNICATION INTERFACE –

Part 2: Functional safety extensions

1 Scope

This part of IEC 61139 specifies the extensions to SDCI in IEC 61131-9 for functional safety. This comprises:

- a standardized OSSDe interface for redundant switching signals based on IEC 61131-2,
- minor modifications/extensions to state machines of SDCI to support the safety operations,
- a lean functional safety communication protocol on top of the standard SDCI communication which is a black channel according to IEC 61784-3:2021,
- protocol management functions for configuration, parameterization, and commissioning,
- IODD extensions for functional safety,
- a Device tool interface to support Dedicated Tools according to functional safety standards.

This document does not cover:

- communication interfaces or systems including multi-point or multi-drop linkages,
- communication interfaces or systems including multi-channel or encrypted linkages,
- wireless communication interfaces or systems,
- integration of SDCI-FS into upper-level systems such as fieldbuses/FSCPs.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60204-1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

IEC 61010-2-201, *Safety requirements for electrical equipment for measurement, control and laboratory use – Part 2-201: Particular requirements for control equipment*

IEC 61131-2, *Industrial-process measurement and control – Programmable controllers – Part 2: Equipment requirements and tests*

IEC 61131-9:—[3], *Programmable controllers – Part 9: Single-drop digital communication interface for small sensors and actuators (SDCI)*

IEC 61496-1, *Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests*

[3] Under preparation. Stage at the time of publication: IEC/CFDIS 61131-9:2022.

IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61784-3:2021, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 62061, *Safety of machinery – Functional safety of safety-related control systems*

IEC 62443 (all parts), *Security for industrial automation and control systems*

ISO 639-2, *Codes for the representation of names of languages – Part 2: Alpha-3 code*

ISO 639-3, *Codes for the representation of names of languages – Part 3: Part 3: Alpha-3 code for comprehensive coverage of languages*

ISO 13849-1, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

SOMMAIRE

AVANT-PROPOS 208
INTRODUCTION 210
1 Domaine d'application 213
2 Références normatives 213
3 Termes, définitions, symboles, termes abrégés et conventions 214
3.1 Termes et définitions 214
3.2 Termes et définitions communs 214
3.3 Termes et définitions relatifs à la SDCI-FS 218
3.4 Symboles et abréviations 219
3.5 Conventions 221
3.5.1 Descriptions comportementales 221
3.5.2 Ordre des octets de mémoire et de transmission 222
4 Présentation de la SDCI-FS 222
4.1 Objet de la technologie et niveaux de fonctionnalité 222
4.1.1 Technologie SDCI-FS de base 222
4.1.2 De "analogique" et "commutation" vers la communication 223
4.1.3 Changement de paradigme réduit de FS-DI à Maître FS 224
4.1.4 Après le paradigme SDCI (SIO/OSSDe) 225
4.1.5 Port de classe B 227
4.1.6 "Maître USB" avec paramétrage de sécurité 228
4.1.7 Matrice d'interopérabilité des appareils de sécurité 228
4.2 Positionnement dans la hiérarchie d'automatisation 229
4.3 Câblage, connecteurs et alimentation 230
4.4 Relation avec la SDCI 230
4.5 Fonctionnalités et interfaces de communication 231
4.6 Paramétrage 231
4.7 Rôle du Maître FS et de la passerelle FS 232
4.8 Mapping vers les systèmes de niveau supérieur 232
4.9 Structure du document 232
5 Extensions de la couche physique (PL) 233
5.1 Vue d'ensemble 233
5.2 Extensions des services PL 234
5.2.1 PL_SetMode 234
5.2.2 PL_Ready 234
5.3 Emetteur/Récepteur 234
5.3.1 Hypothèses pour l'extension vers OSSDe 234
5.3.2 Spécificités OSSDe 235
5.3.3 Démarrage d'un Appareil FS (impulsion Ready) 238
5.3.4 Caractéristiques électriques d'un récepteur dans l'Appareil FS et le Maître FS 238
5.4 Caractéristiques électriques et dynamiques d'un Appareil FS 239
5.5 Caractéristiques électriques et dynamiques d'un port de Maître FS (OSSDe) 242
5.6 Interface FS-DI du port du Maître FS 244
5.7 Coordination de la réactivation 244
5.8 Démarrage rapide 245
5.9 Alimentation 245
5.10 Support 246

5.10.1 Contraintes 246
5.10.2 Connecteurs 246
5.10.3 Caractéristiques des câbles 246
6 Extensions du mode SIO 246
7 Extensions de la couche de liaison de données (DL) 246
7.1 Vue d'ensemble 246
7.2 Diagramme d'états du gestionnaire de mode DL du Maître FS 246
7.3 Diagramme d'états du gestionnaire de mode DL de l'Appareil FS 248
8 Extensions du gestionnaire de configuration (CM) du Maître 250
9 Extensions de l'Appareil FS 251
9.1 Architecture de principe et modèles 251
9.1.1 Architecture de l'Appareil FS 251
9.1.2 Modèle de l'Appareil FS 252
9.2 Gestionnaire de paramètres (PM) 253
9.3 Echange des données de processus (PDE) 253
9.4 Stockage de données (DS) 254
9.4.1 Considérations générales et extensions, y compris de sécurité 254
9.4.2 Niveaux de sauvegarde 254
10 Extensions du Maître FS 255
10.1 Architecture de principe 255
10.2 Extensions des services SMI 256
10.2.1 Vue d'ensemble 256
10.2.2 SMI_FSMasterAccess 257
10.2.3 SMI_SPDUIn 259
10.2.4 SMI_SPDUOut 259
10.2.5 SMI_FSPDInOut 259
10.3 Extensions d'ArgBlock 261
10.3.1 Vue d'ensemble 261
10.3.2 FSMasterAccess 262
10.3.3 FSCPAuthenticity 262
10.3.4 FSPortConfigList 262
10.3.5 FSPortStatusList 265
10.3.6 SPDUIn 267
10.3.7 SPDUOut 267
10.3.8 FSPDInOut 268
10.4 Gestionnaire de couche de sécurité (SLM) 269
10.4.1 Objet 269
10.4.2 FS_PortMode 269
10.4.3 Paramètre FSP 269
10.5 Echange des données de processus (PDE) 273
10.6 Stockage de données (DS) 274
11 Couche de communication de sécurité (SCL) 274
11.1 Exigences fonctionnelles 274
11.2 Erreurs de communication et mesures de sécurité 274
11.3 Services SCL 275
11.3.1 Positionnement des couches de communication de sécurité (SCL) 275
11.3.2 Services SCL du Maître FS 276
11.3.3 Services SCL de l'Appareil FS 278

11.4 Protocole SCL 280
11.4.1 Phases de protocole à prendre en compte 280
11.4.2 Anomalies de l'Appareil FS 281
11.4.3 PDU de sécurité (SPDU) 282
11.4.4 Données d'entrée FS et de sortie FS 282
11.4.5 Numéro de port 282
11.4.6 Etat et contrôle 282
11.4.7 Signature CRC 283
11.4.8 Considérations de sécurité relatives à l'opportunité, l'authenticité et l'intégrité des données ("TADI") (informative) 284
11.4.9 Types de données pour SDCI-FS 285
11.5 Comportement SCL 287
11.5.1 Généralités 287
11.5.2 Diagramme d'états SCL du Maître FS 287
11.5.3 Diagramme d'états SCL de l'Appareil FS 290
11.5.4 Diagrammes séquentiels pour plusieurs cas d'utilisation 293
11.5.5 Surveillance des temps de sécurité 299
11.5.6 Réaction en cas de dysfonctionnement 300
11.5.7 Démarrage (communication) 302
11.6 Gestion de la SCL 303
11.6.1 Vue d'ensemble des paramètres (FSP et FST) 303
11.6.2 Approches de paramétrage 304
11.7 Mesures d'intégrité 305
11.7.1 Intégrité de l'IODD 305
11.7.2 Intégrité des outils 305
11.7.3 Intégrité de la transmission 306
11.7.4 Enregistrement de vérification 306
11.7.5 Authentification 306
11.7.6 Intégrité du stockage 306
11.7.7 Intégrité de la structure de données d'E/S FS 307
11.7.8 Paramètres de technologie (FST) fondés sur l'IODD 308
11.7.9 Paramètres de technologie (FST) fondés sur un outil dédié existant (IOPD) 309
11.8 Création des paramètres FSP et FST 309
11.9 Intégration des outils dédiés (IOPD) 310
11.9.1 Interface IOPD 310
11.9.2 Interfaces normalisées 311
11.9.3 Canal de retour 311
11.10 Validation 312
11.11 Passivation 312
11.11.1 Motifs et moyens 312
11.11.2 Passivation sélective du port (Maître FS) 313
11.11.3 Passivation sélective du signal (borne FS) 313
11.11.4 Réglages des qualificatifs en cas de communication 313
11.11.5 Gestion des qualificatifs en cas d'OSSDe 314
11.12 Diagnostic SCL 315
12 Traitement de sécurité fonctionnelle (FS-P) 315
12.1 Recommandations pour des mappings d'E/S efficaces 315
12.2 Contrôleur FS intégré 316

Annexe A (normative) Extensions des paramètres 317
A.1 Index et paramètres pour SDCI-FS 317
A.2 Détail des paramètres 318
A.2.1 FSP_Authenticity 318
A.2.2 FSP_Port 319
A.2.3 FSP_AuthentCRC 319
A.2.4 FSP_ProtVersion 319
A.2.5 FSP_ProtMode 319
A.2.6 FSP_Watchdog 320
A.2.7 FSP_IO_StructCRC 320
A.2.8 FSP_TechParCRC 321
A.2.9 FSP_ProtParCRC 321
A.2.10 FSP_VerifyRecord 322
A.2.11 FSP_TimeToReady 322
A.2.12 FSP_MinShutDownTime 322
A.2.13 FSP_WCDT 322
A.2.14 FSP_OFDT 322
A.2.15 FSP_ParamDescCRC 322
Annexe B (normative) Extensions des EventCodes 324
B.1 EventCodes d'Appareil FS supplémentaires 324
B.2 EventCodes de port supplémentaires 324
Annexe C (normative) Extensions des types de données 326
C.1 Types de données pour SDCI-FS 326
C.2 BooleanT (bit) 326
C.3 IntegerT (16) 327
C.4 IntegerT (32) 327
C.5 Code de sécurité 328
Annexe D (normative) Polynômes générateurs de CRC 330
D.1 Vue d’ensemble des polynômes générateurs de CRC 330
D.2 Probabilités d'erreurs résiduelles 331
D.3 Considérations relatives à la mise en œuvre 332
D.3.1 Vue d’ensemble 332
D.3.2 Algorithme de décalage de bits (16 bits) 332
D.3.3 Table de conversion (16 bits) 333
D.3.4 Algorithme de décalage de bits (32 bits) 334
D.3.5 Table de conversion (32 bits) 335
D.3.6 Valeurs de départ 336
D.3.7 Ordre des octets pour le calcul de la CRC 337
Annexe E (normative) Extensions de l'IODD 338
E.1 Généralités 338
E.2 Schéma 338
E.3 Contraintes de l'IODD 338
E.3.1 Règles générales 338
E.3.2 Description de la structure de l'IODD 338
E.3.3 Comportement des SystemCommands "Reset" dans la SDCI-FS 345
E.3.4 Caractéristiques de profil 346
E.3.5 ProcessDataInput et ProcessDataOutput 346
E.4 Conventions IODD 346

E.4.1 Nommage 346
E.4.2 Données de processus (PD) 346
E.4.3 Conventions IODD pour l'interface utilisateur 347
E.4.4 Fonctionnalités des outils du Maître 347
E.5 Sécurisation 347
E.5.1 Généralités 347
E.5.2 DefaultValues pour FSP 348
E.5.3 FSP_Authenticity 348
E.5.4 FSP_Protocol 348
E.5.5 FSP_IO_Description 349
E.5.6 Exemple de sérialisation pour FSP_ParamDescCRC 349
E.5.7 Paramètres FST et FSP et stockage de données 350
E.5.8 Exemple d'IODD d'un Appareil FS 351
Annexe F (normative) Interface d'outil d'Appareil (DTI) pour SDCI 361
F.1 Objet de la DTI 361
F.2 Modèle de base 361
F.3 Interface d'appel 362
F.3.1 Vue d'ensemble 362
F.3.2 Détection de l'outil d'Appareil 363
F.3.3 Description d'interface de programme (PID) 366
F.3.4 Fichier de paramètres temporaire (TPF) 370
F.3.5 Fichier de backchannel temporaire (TBF) 375
F.3.6 Fichier d'acquittement temporaire (TAF) 377
F.3.7 Comportement d'appel 377
F.4 Objets de données d'Appareil (DDO) 378
F.4.1 Généralités 378
F.4.2 Structure d'un paquet DDO 379
F.5 Interface de communication 379
F.5.1 Généralités 379
F.5.2 Principe des communications DTI 380
F.5.3 Passerelles 382
F.5.4 Configuration du serveur de communication 382
F.5.5 Définition de l'interface de communication 382
F.5.6 Séquence d'établissement d'une relation de communication 382
F.5.7 Utilisation du serveur de communication en mode autonome 384
F.5.8 Spécificités de la SDCI 384
F.5.9 Modification des paramètres de communication 385
F.6 Réaction en cas de comportement incorrect de l'outil 385
F.7 Compatibilité 386
F.7.1 Validation du schéma 386
F.7.2 Politique relative aux versions 386
F.8 Evolutivité 387
F.8.1 Evolutivité d'un outil d'Appareil 387
F.8.2 Evolutivité d'un outil de Maître 387
F.8.3 Interactions selon les combinaisons de classes de conformité 388
F.9 Définitions des schémas 388
F.9.1 Généralités 388
F.9.2 Schéma du PID 388
F.9.3 Schéma du TPF 390

F.9.4 Schéma du TBF 392
F.9.5 Schéma du TAF 393
F.9.6 Schéma des primitives DTI 394
Annexe G (normative) Principaux scénarios de SDCI-FS 396
G.1 Vue d'ensemble 396
G.2 Diagramme séquentiel de mise en service 397
G.3 Diagramme séquentiel de remplacement 398
G.4 Diagramme séquentiel de mauvaise connexion 399
Annexe H (normative) Exigences système 400
H.1 Indicateurs 400
H.1.1 Généralités 400
H.1.2 OSSDe 400
H.1.3 Communication de sécurité 400
H.1.4 Demande d'acquittement 400
H.2 Lignes directrices relatives à l'installation, sûreté électrique et sécurité 400
H.3 Temps de réponse de la fonction de sécurité 401
H.4 Durée des demandes (ou sollicitations) 401
H.5 Maintenance et réparation 401
H.6 Manuel de sécurité 401
Annexe I (informative) Informations pour l'essai et l'évaluation des composants SDCI-FS 403
Bibliographie 404

Figure 1 – Positionnement de la SDCI-FS pour l'automatisation de sécurité fonctionnelle 211
Figure 2 – Relations du présent document avec les normes 212
Figure 3 – Ordre des octets de mémoire et de transmission 222
Figure 4 – Modèle de couche de communication SDCI-FS 222
Figure 5 – Extensions d'interface de port pour SDCI-FS 223
Figure 6 – Migration vers une SDCI-FS 224
Figure 7 – Changement de paradigme réduit de FS-DI à Maître FS 225
Figure 8 – Types de Maîtres FS et niveaux de fonctionnalité 225
Figure 9 – Disposition d'origine des broches de la SDCI (ports de classe A) 226
Figure 10 – Mise en service OSSDe optimisée avec un Maître FS 227
Figure 11 – Niveau "d" d'un Maître FS (classe B) 228
Figure 12 – Configuration et paramétrage hors site 228
Figure 13 – SDCI-FS dans la hiérarchie d'automatisation 230
Figure 14 – Couche physique SDCI d'un Maître FS (classe A) 233
Figure 15 – Couche physique d'un Appareil FS (classe A) 233
Figure 16 – Compatibilité transversale entre OSSD et OSSDe 234
Figure 17 – Principe de fonctionnement OSSDe 235
Figure 18 – Impulsions d'essai pour détecter les anomalies d'interconnexion 237
Figure 19 – Temporisations OSSD 237
Figure 20 – Démarrage type d'un capteur OSSD 238
Figure 21 – Démarrage d'un Appareil FS 238

Figure 22 – Seuils de commutation pour les récepteurs de l'Appareil FS et du Maître FS 239
Figure 23 – Schéma de référence (un canal OSSDe) 240
Figure 24 – Définitions des niveaux de tension 240
Figure 25 – Capacité de charge à la mise sous tension 244
Figure 26 – Résolution du conflit avec le filtre d'entrée OSSDe 244
Figure 27 – Démarrage d'un Appareil FS 245
Figure 28 – Temporisations de démarrage rapide exigées 245
Figure 29 – Diagramme d'états du gestionnaire de mode DL du Maître FS 247
Figure 30 – Diagramme d'états du gestionnaire de mode DL de l'Appareil FS 249
Figure 31 – Extension du gestionnaire de configuration (VerifyRecord) 250
Figure 32 – Architecture de principe de l'Appareil FS 252
Figure 33 – Modèle de l'Appareil FS 253
Figure 34 – Architecture de principe du Maître FS 255
Figure 35 – Extensions des services SMI 257
Figure 36 – Cas d'utilisation des paramètres FSP 270
Figure 37 – Séparateur PDE 273
Figure 38 – Compositeur PDE 274
Figure 39 – Positionnement de la couche de communication de sécurité SDCI-FS (SCL) 276
Figure 40 – Services de la couche de communication de sécurité du Maître FS 277
Figure 41 – Services de la couche de communication de sécurité de l'Appareil FS 279
Figure 42 – Phases de protocole à prendre en compte 281
Figure 43 – PDU de sécurité du Maître FS et de l'Appareil FS 282
Figure 44 – Règle du taux de 1 % de l'IEC 61784-3:2021 284
Figure 45 – Diagramme d'états SCL du Maître FS 287
Figure 46 – Diagramme d'états SCL de l'Appareil FS 290
Figure 47 – Maître FS et Appareil FS tous deux sous tension (ON) 293
Figure 48 – Maître FS hors tension puis sous tension (OFF → ON) 294
Figure 49 – Appareil FS avec démarrage SCL différé 295
Figure 50 – Appareil FS hors tension puis sous tension (OFF -> ON) 296
Figure 51 – Détection d'une erreur de signature CRC par le Maître FS 297
Figure 52 – Détection d'une erreur de signature CRC par l'Appareil FS 298
Figure 53 – Surveillance de la durée de cycle SCL 299
Figure 54 – Types de paramètres et affectations 304
Figure 55 – Système centré sur l'hôte FSCP 305
Figure 56 – Structure de FSP_VerifyRecord 306
Figure 57 – Démarrage de la SDCI-FS 307
Figure 58 – Sécurisation des paramètres FST avec un outil dédié 308
Figure 59 – Modification des paramètres FST avec un outil d'Appareil 309
Figure 60 – Création des paramètres FSP et FST 310
Figure 61 – Exemple de hiérarchie de communication 311
Figure 62 – Motifs de la passivation sélective du port 312
Figure 63 – Gestionnaire de qualificatifs (communication) 313

Figure 64 – Gestionnaire de qualificatifs (OSSDe) 314
Figure 65 – Comportement des qualificatifs par port du Maître FS 314
Figure 66 – Problèmes liés à l'efficacité du mapping 316
Figure A.1 – Instance d'une description des données d'E/S FS 321
Figure A.2 – Exemple de structure de données d'E/S FS avec des données non relatives à la sécurité 321
Figure A.3 – Sécurisation des paramètres de sécurité 323
Figure C.1 – Exemple de structure de données BooleanT 327
Figure C.2 – Code de sécurité d'un message de sortie 328
Figure C.3 – Code de sécurité d'un message d'entrée 329
Figure D.1 – Polynôme générateur de CRC-16 331
Figure D.2 – Polynôme générateur de CRC-32 332
Figure D.3 – Algorithme de décalage de bits en langage "C" (16 bits) 333
Figure D.4 – Calcul de la signature CRC-16 à l'aide d'une table de conversion 333
Figure D.5 – Algorithme de décalage de bits en langage "C" (32 bits) 335
Figure D.6 – Calcul de la signature CRC-32 à l'aide d'une table de conversion 335
Figure E.1 – Algorithme de génération des signatures CRC des paramètres FSP 348
Figure F.1 – Principe de l'interface d'appel DTI 362
Figure F.2 – Structure du registre 363
Figure F.3 – Exemple de registre DTI 364
Figure F.4 – Détection d'un outil d'Appareil dans le registre 366
Figure F.5 – Menu pour appeler l'outil d'Appareil 367
Figure F.6 – Objectif des objets de données d'Appareil (DDO) 379
Figure F.7 – Voies de communication entre l'outil d'Appareil et l'Appareil 380
Figure F.8 – Routage sur les réseaux et la SDCI 381
Figure F.9 – Serveur de communication 381
Figure F.10 – Diagramme séquentiel pour l'établissement d'une communication 383
Figure F.11 – Création d'une instance de serveur de communication 383
Figure F.12 – Exemple de document XML ConnectRequest pour SDCI 385
Figure F.13 – Schéma XML du fichier PID 388
Figure F.14 – Schéma XML du TPF 390
Figure F.15 – Schéma XML d'un TBF 392
Figure G.1 – Mise en service avec essai et fonctionnement armé 398
Figure G.2 – Remplacement d'Appareil FS 399
Figure G.3 – Mauvaise connexion d'Appareil FS 399

Tableau 1 – Modes opérationnels des niveaux de fonctionnalité "a" à "c" (ports de classe A) 227
Tableau 2 – Matrice d'interopérabilité des appareils de sécurité 229
Tableau 3 – PL_Ready 234
Tableau 4 – Etats et conditions OSSD 236
Tableau 5 – Anomalies d'interconnexion 236
Tableau 6 – Caractéristiques électriques d'un récepteur 239
Tableau 7 – Caractéristiques électriques et dynamiques d'un Appareil FS (OSSDe) 241

Tableau 8 – Caractéristiques électriques et dynamiques de l'interface du port 243
Tableau 9 – Caractéristiques des câbles 246
Tableau 10 – Tableaux de transition d'états du gestionnaire de mode DL du Maître FS 248
Tableau 11 – Tableaux de transition d'états du gestionnaire de mode DL de l'Appareil FS 249
Tableau 12 – Tableaux de transition d'états du gestionnaire de configuration 251
Tableau 13 – Extension du diagramme d'états de stockage de données (DS) 254
Tableau 14 – Niveaux de sauvegarde du stockage de données 254
Tableau 15 – Services SMI utilisés pour le Maître FS 256
Tableau 16 – SMI_FSMasterAccess 258
Tableau 17 – SMI_FSPDInOut 260
Tableau 18 – Types d'ArgBlocks et ArgBlockIDs 261
Tableau 19 – FSMasterAccess 262
Tableau 20 – FSCPAuthenticity 262
Tableau 21 – FSPortConfigList 263
Tableau 22 – FSPortStatusList 266
Tableau 23 – SPDUIn 267
Tableau 24 – SPDUOut 268
Tableau 25 – FSPDInOut 268
Tableau 26 – Tableau de référence des cas d'utilisation 270
Tableau 27 – Erreurs de communication et mesures de sécurité 275
Tableau 28 – Services SCL du Maître FS 278
Tableau 29 – Services SCL de l'Appareil FS 280
Tableau 30 – Phases de protocole à prendre en compte 281
Tableau 31 – Contrôle et comptage (Control&MCnt) 283
Tableau 32 – Etat et comptage en miroir (Status&DCnt) 283
Tableau 33 – Valeurs MCount et DCount_i 283
Tableau 34 – Types de données d'E/S de processus FS 286
Tableau 35 – Règles de disposition des valeurs et des qualificatifs 286
Tableau 36 – Ordre des valeurs et des qualificatifs 286
Tableau 37 – Définition des termes utilisés dans le diagramme d'états SCL du Maître FS 288
Tableau 38 – Etats et transitions SCL du Maître FS 288
Tableau 39 – Définition des termes utilisés dans le diagramme d'états SCL de l'Appareil FS 290
Tableau 40 – Etats et transitions SCL de l'Appareil FS 291
Tableau 41 – Contraintes de temporisation 299
Tableau 42 – Bits qualificatifs "GOOD/BAD" 313
Tableau 43 – Tableaux de transition d'états pour le comportement des qualificatifs 315
Tableau A.1 – Index pour SDCI-FS 317
Tableau A.2 – Codage de la version de protocole 319
Tableau A.3 – Codage du mode de protocole 319
Tableau A.4 – Description de la structure de données d'E/S FS générique 320
Tableau B.1 – EventCodes spécifiques à la SCL de l'Appareil FS 324

Tableau B.2 – EventCodes spécifiques à la SCL du Maître FS 325
Tableau C.1 – Types de données pour SDCI-FS 326
Tableau C.2 – BooleanT pour SDCI-FS 326
Tableau C.3 – Exemple de BooleanT dans un RecordT 326
Tableau C.4 – IntegerT(16) 327
Tableau C.5 – Codage d'IntegerT(16) 327
Tableau C.6 – IntegerT(32) 328
Tableau C.7 – Codage d'IntegerT(32) 328
Tableau D.1 – Polynômes générateurs de CRC pour SDCI-FS 330
Tableau D.2 – Définition des variables utilisées à la Figure D.3 333
Tableau D.3 – Définition des variables utilisées à la Figure D.4 333
Tableau D.4 – Table de conversion pour le calcul de la signature CRC-16 334
Tableau D.5 – Définition des variables utilisées à la Figure D.5 335
Tableau D.6 – Définition des variables utilisées à la Figure D.4 335
Tableau D.7 – Table de conversion pour le calcul de la signature CRC-32 336
Tableau E.1 – Comportement spécifique des SystemCommands "Reset" de l'Appareil FS 346
Tableau E.2 – Actions utilisateur pour remplacer les DefaultValue 348
Tableau E.3 – RecordItems de FSP_Protocol dont les valeurs admises doivent être sérialisées 349
Tableau E.4 – Exemple de sérialisation pour FSP_ParamDescCRC 349
Tableau F.1 – Description des éléments du fichier PID 367
Tableau F.2 – Eléments du TPF 370
Tableau F.3 – Eléments du TBF 376
Tableau F.4 – Eléments du TAF 377
Tableau F.5 – Cas et comportements d'appel 378
Tableau F.6 – Mapping du schéma de communication 384
Tableau F.7 – Réaction en cas de comportement incorrect de l'outil 386
Tableau F.8 – Classes de conformité DTI 387
Tableau F.9 – Niveaux de fonctionnalité DTI des outils d'Appareil 387
Tableau F.10 – Interactions selon les combinaisons de classes de conformité 388
Tableau G.1 – Principaux scénarios de SDCI-FS 396

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX INDUSTRIELS – INTERFACE DE COMMUNICATION NUMÉRIQUE POINT À POINT –

Partie 2: Extensions de sécurité fonctionnelle

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 61139-2 a été établie par le sous-comité 65C: Réseaux industriels, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels. Il s'agit d'une Norme internationale.

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
65C/1168/FDIS	65C/1174/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/standardsdev/publications.

Une liste de toutes les parties de la série IEC 61139, publiées sous le titre général *Réseaux industriels – Interface de communication numérique point à point*, se trouve sur le site web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

La technologie de base IO-Link™[1] est l'objet de la Norme internationale IEC 61131-9, qui fait partie d'une série de normes sur les automates programmables et les périphériques associés, tels que les systèmes d'E/S déportés (RIO).

Elle spécifie une technologie d'interface de communication numérique point à point (appelée SDCI, *Single-drop Digital Communication Interface*), qui étend les interfaces d'entrée et de sortie de commutation traditionnelles définies dans l'IEC 61131-2 vers une liaison de communication point à point qui utilise une commutation codée. Cette technologie permet l'échange cyclique de données de processus d'entrée et de sortie numériques entre un Maître et ses Appareils associés (capteurs, actionneurs, bornes d'E/S, etc.). Le Maître peut faire partie d'un système de communication par bus de terrain ou de toute unité de traitement autonome. La technologie permet également le transfert acyclique de paramètres vers les Appareils et la propagation d'informations de diagnostic des Appareils vers le système d'automatisation de niveau supérieur (contrôleur, hôte) par l'intermédiaire du Maître.

La topologie physique point à point entre chaque Appareil et le Maître utilise 3 fils sur des distances inférieures ou égales à 20 m. L'interface physique SDCI est rétrocompatible avec la signalisation d'E/S 24 V habituelle spécifiée dans l'IEC 61131-2 et prend en charge trois taux de transmission, de 4,8 kbit/s, 38,4 kbit/s et 230,4 kbit/s.

Les principaux avantages de la technologie SDCI sont les suivants:

- double utilisation des communications à signaux de commutation (DI/DO) ou à commutation codée, respectivement;
- les capteurs et les actionneurs de commutation traditionnels fournissent désormais, en variante, une communication numérique point à point au sein d'un même Appareil;
- un câble fin, robuste et très souple, sans blindage, pour l'alimentation et la signalisation;
- communication numérique à moindre coût, jusqu'aux moindres capteurs et actionneurs.

La variante de sécurité fonctionnelle de la SDCI est appelée SDCI-FS. La Figure 1 représente un exemple de positionnement de la SDCI-FS pour l'automatisation de sécurité fonctionnelle.

---

[1] IO-Link™ est le nom commercial de la communauté IO-Link. Cette information est donnée à l'intention des utilisateurs de la présente spécification et ne signifie nullement que la communauté IO-Link approuve ou recommande le détenteur de la marque ou de l'un de ses produits. La conformité au présent document n'exige pas l'emploi des logos déposés pour IO-Link™. L'emploi des logos déposés pour IO-Link™ exige l'autorisation de la communauté IO-Link.

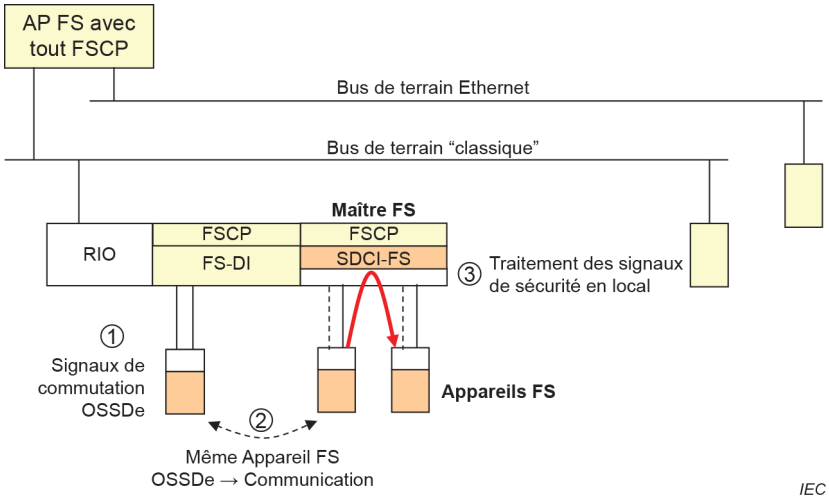


Figure 1 – Positionnement de la SDCI-FS pour l'automatisation de sécurité fonctionnelle

Dans cet exemple, un système d'E/S déporté est connecté à un automate programmable de sécurité fonctionnelle par l'un des FSCP de la série IEC 61784-3 [1][2] pour communiquer avec un module FS-DI et une passerelle vers un Maître FS SDCI-FS. Les Appareils FS avec OSSDe peuvent être connectés à des FS-DI ou à des Maîtres FS. Tous les Appareils FS peuvent communiquer avec tout Maître FS en utilisant le protocole SDCI-FS, quel que soit le système FSCP de niveau supérieur. Il en va de même pour les actionneurs de sécurité (Appareils FS) tels que les commandes à sécurité intégrée. Cela implique une plus grande uniformité des composants ① pour les capteurs et les actionneurs, similaire aux interfaces DI et DO normalisées dans le cadre de l'IEC 61131-2.

Les capteurs de sécurité avec interfaces OSSDe (équipés d'un système de communication SDCI-FS) peuvent être paramétrés par l'intermédiaire d'outils auxiliaires, tels que des "Maîtres USB", puis connectés à un FS-DI et utilisés en mode OSSDe. Ils peuvent également être utilisés en mode OSSDe sur un Maître FS qui prend en charge OSSDe. Si ces capteurs de sécurité sont équipés d'un système de communication SDCI-FS supplémentaire, ils peuvent être utilisés dans les deux modes ②, OSSDe ou SDCI-FS. Cela correspond au paradigme SIO SDCI.

Le concept de SDCI-FS permet le traitement des signaux de sécurité en local si la passerelle/le Maître FS fournit un contrôleur de sécurité local ③.

Le présent document fournit les extensions nécessaires à l'IEC 61131-9 pour la communication de sécurité fonctionnelle, y compris la normalisation de l'OSSDe et le paramétrage dans le domaine de la sécurité des machines. La Figure 2 représente les relations avec les Normes internationales de bus de terrain et de sécurité, ainsi qu'avec les spécifications applicables (voir Article 2 et Bibliographie). Toute sécurité fonctionnelle commence par l'appréciation du risque et la réduction du risque (ISO 12100). Une possibilité de réduction du risque consiste à utiliser des systèmes de commande électriques ou électroniques. Pour la conception de ces derniers, des normes telles que l'IEC 61508, l'IEC 62061 et l'ISO 13849 peuvent être utilisées. Les conditions d'environnement, comme la CEM, sont couvertes, par exemple, par l'IEC 61000-6-7. D'autres aspects concernent les installations et les questions de sécurité. Plusieurs normes de produits, telles que l'IEC 60947-5-3 et l'ISO 14119, complètent les normes génériques ou sectorielles.

2 Les chiffres entre crochets renvoient à la Bibliographie.

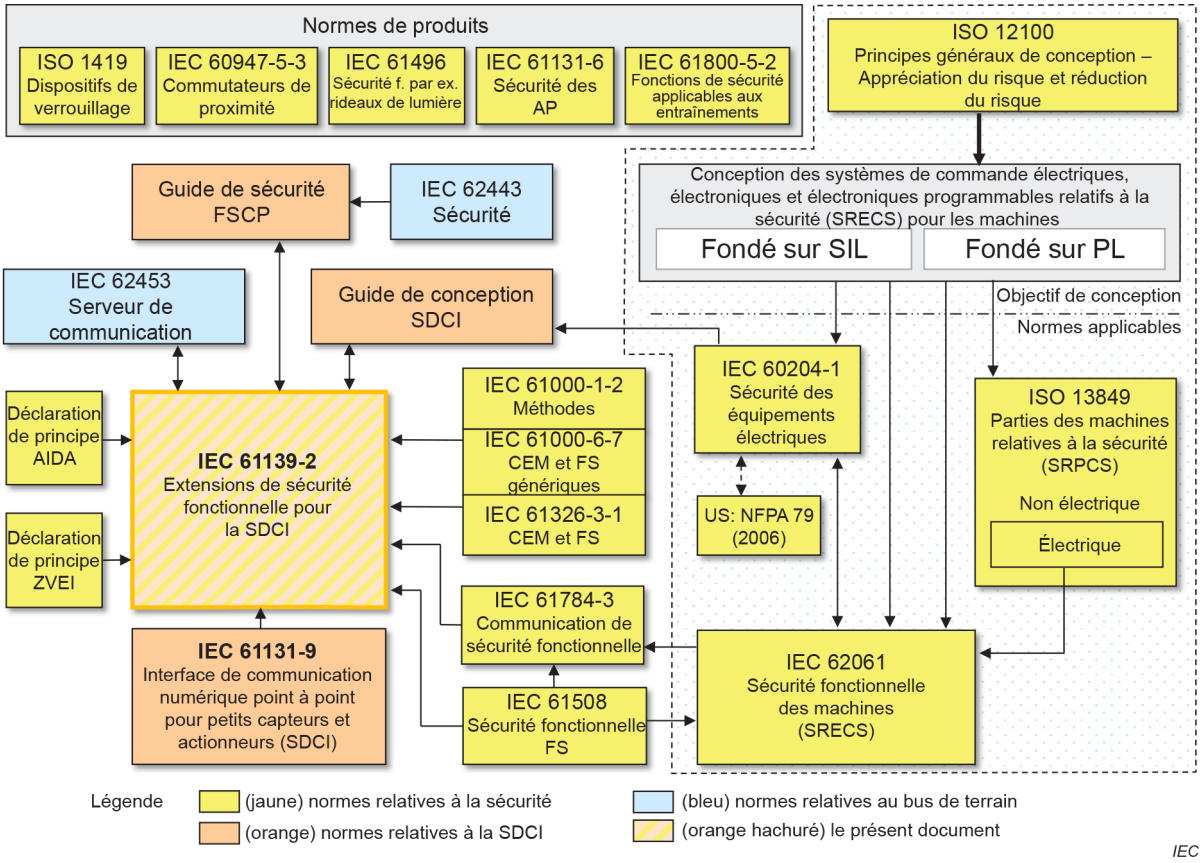


Figure 2 – Relations du présent document avec les normes

La SDCI-FS peut être utilisée pour les applications de sécurité fonctionnelle selon l'IEC 62061 et l'IEC 61508 jusqu'à SIL3 et/ou selon l'ISO 13849 jusqu'à PLe.

RÉSEAUX INDUSTRIELS – INTERFACE DE COMMUNICATION NUMÉRIQUE POINT À POINT –

Partie 2: Extensions de sécurité fonctionnelle

1 Domaine d'application

La présente partie de l'IEC 61139 spécifie les extensions de la SDCI de l'IEC 61131-9 pour la sécurité fonctionnelle. Elle comprend:

- une interface OSSDe normalisée pour les signaux de commutation redondants, fondée sur l'IEC 61131-2;
- des modifications/extensions mineures des diagrammes d'états de la SDCI afin de prendre en charge les opérations de sécurité;
- un protocole de communication de sécurité fonctionnelle affiné en plus de la communication SDCI normalisée, qui constitue un canal noir selon l'IEC 61784-3:2021;
- des fonctions de gestion de protocole pour la configuration, le paramétrage et la mise en service;
- des extensions de l'IODD pour la sécurité fonctionnelle;
- une interface d'outil d'Appareil pour prendre en charge les outils dédiés, conformément aux normes de sécurité fonctionnelle.

Le présent document ne couvre pas:

- les interfaces ou systèmes de communication qui incluent des liaisons multipoints;
- les interfaces ou systèmes de communication qui incluent des liaisons chiffrées ou multicanaux;
- les interfaces ou systèmes de communication sans fil;
- l'intégration de la SDCI-FS aux systèmes de niveau supérieur, tels que les bus de terrain/FSCP.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60204-1, *Sécurité des machines – Equipement électrique des machines – Partie 1: Exigences générales*

IEC 61010-2-201, *Exigences de sécurité pour appareils électriques de mesurage, de régulation et de laboratoire – Partie 2-201: Exigences particulières relatives aux équipements de commande*

IEC 61131-2, *Mesure et commande des processus industriels – Automates programmables – Partie 2: Spécifications et essais des équipements*

IEC 61131-9:—[3], *Automates programmables – Partie 9: Interface de communication numérique point à point pour petits capteurs et actionneurs (SDCI)*

IEC 61496-1, *Sécurité des machines – Equipements de protection électrosensibles – Partie 1: Exigences générales et essais*

IEC 61508-3, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*

IEC 61784-3:2021, *Réseaux de communication industriels – Profils – Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profils*

IEC 62061, *Sécurité des machines – Sécurité fonctionnelle des systèmes de commande relatifs à la sécurité*

IEC 62443 (toutes les parties), *Sécurité des systèmes d'automatisation et de commande industriels*

ISO 639-2, *Codes pour la représentation des noms de langue – Partie 2: Code alpha-3*

ISO 639-3, *Codes pour la représentation des noms de langue – Partie 3: Partie 3: Code alpha-3 pour un traitement exhaustif des langues*

ISO 13849-1, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception*

---

[3] En cours d'élaboration. Stade au moment de la publication: IEC/CFDIS 61131-9:2022.